## AMENDMENTS TO THE CLAIMS

Applicant submits below a complete listing of the current claims, including marked-up claims with insertions indicated by underlining and deletions indicated by strikeouts and/or double bracketing. This listing of claims replaces all prior versions, and listings, of claims in the application:

### Listing of the Claims

1. (Original) A method of wirelessly generating a cryptographic key that may be used to encrypt wireless communications between a first host and a second host, the method comprising the steps of:

selecting an initial modulation scheme for wireless transmission between the first host and the second host;

transmitting via the initial modulation scheme first data to be used in generating the cryptographic key and an indication of a second modulation scheme;

receiving via the second modulation scheme second data to be used in generating the cryptographic key; and

generating the cryptographic key using the first and the second data.

2. (Original) The method of claim 1, wherein the step of receiving further comprises the step of:

receiving via the second modulation scheme an indication of a third modulation scheme, the method further comprising the steps of:

transmitting via the third modulation scheme third data to be used in generating the cryptographic key and an indication of a fourth modulation scheme;

receiving via the fourth modulation scheme fourth data to be used in generating the cryptographic key; and

wherein the step of:

generating the cryptographic key using the first and the second data further comprises the step of:

generating the cryptographic key using the first, second, third, and fourth data.

3. (Original) The method of claim 1, further comprising the steps of:

determining a desired modulation scheme for wireless communications between the first host and the second host;

encrypting wireless data to be transmitted using the cryptographic key; and

transmitting the encrypted wireless data via the desired modulation scheme.

4. (Original) The method of claim 1, further comprising the steps of:

determining a size of the cryptographic key;

monitoring an amount of data exchanged; and

selecting a final modulation scheme for a final data exchange between the first host and the second host such that an amount of data conveyed by the final modulation scheme added to the amount of data exchanged equals the size of the cryptographic key.

5. (Original) The method of claim 1, wherein the step of:

selecting an initial modulation scheme comprises the step of sharing a short key established by a public key method, the short key providing an index to the initial modulation scheme.

6. (Original) The method of claim 5, wherein the step of:

sharing a short key established by a public key method comprises the step of sharing a short key established by a Diffie-Hellman key exchange method.

7. (Original) The method of claim 5, wherein the step of:

sharing a short key established by a public key method comprises the step of sharing a short key established using Kerberos.

8. (Original) The method of claim 1, wherein the step of:

selecting an initial modulation scheme comprises the step of selecting an initial constellation.

9. (Original) The method of claim 1, wherein the step of:

selecting an initial modulation scheme comprises the step of selecting an initial bit assignment for a constellation.

10. (Original) A method of wirelessly generating a cryptographic key that may be used to encrypt wireless communications between a first host and a second host, the method comprising the steps of:

transmitting data between the first host and the second host using varying modulation schemes for each transmission; and generating the cryptographic key from the data.

11. (Original) The method of claim 10, wherein the step of transmitting data comprises the step of:

transmitting data and an indication of a next modulation scheme to be used for a next transmission between the first host and the second host.

12. (Original) The method of claim 11, further comprising the steps of:

receiving modulated information; and

demodulating the modulated information via the next modulation scheme to extract the data.

13. (Original) The method of claim 12, wherein the step of demodulating comprises the step of:

demodulating the modulated information via the next modulation scheme to extract the data and an indication of a subsequent modulation scheme to be used for a subsequent transmission between the first host and the second host.

14. (Original) The method of claim 13, further comprising the steps of:

transmitting data between the first host and the second host using the subsequent modulation scheme.

15. (Original) The method of claim 10, further comprising the step of:

determining, between the first host and the second host, an initial modulation scheme for an initial transmission of data between the first host and the second host.

16. (Original) The method of claim 15, wherein the step of determining comprises the step of:

sharing a short key established by a public key method, the short key providing an index to the initial modulation scheme.

17. (Original) The method of claim 10, further comprising the steps of:

determining a length of the cryptographic key to be generated;

tracking an amount of data exchanged between the first host and the second host;

calculating a difference between the length of the cryptographic key and the amount of data exchanged; and

selecting a final modulation scheme for a final transmission of data based on the difference.

18. (Original) The method of claim 17, wherein the step of:

selecting a final modulation scheme for a final transmission of data based on the difference comprises the steps of:

determining an amount of data conveyed by each modulation scheme; and

selecting the final modulation scheme such that the amount of data conveyed by the final modulation scheme equals the difference.

19. (Original) The method of claim 10, further comprising the steps of:

encrypting information to be exchanged wirelessly between the first host and the second host using the cryptographic key;

selecting an optimized modulation scheme for wireless exchange of the information; and

exchanging the encrypted information using the optimized modulation scheme.

20-24. (Canceled)

25. (Currently amended) A ~~computer-readable~~ computer storage medium having computer-executable instructions for, when executed, performing steps, comprising:

selecting an initial modulation scheme for wireless transmission between a first host and a second host;

transmitting via the initial modulation scheme first data to be used in generating a cryptographic key and an indication of a second modulation scheme;

receiving via the second modulation scheme second data to be used in generating the cryptographic key; and

generating the cryptographic key using the first and the second data.

26. (Currently amended) The ~~computer-readable~~ computer storage medium of claim 25, wherein the step of receiving further comprises the step of:

receiving via the second modulation scheme an indication of a third modulation scheme, and wherein the computer-executable instructions further comprise the steps of:

transmitting via the third modulation scheme third data to be used in generating the cryptographic key; and

an indication of a fourth modulation scheme;

receiving via the fourth modulation scheme fourth data to be used in generating the cryptographic key; and

wherein the step of:

generating the cryptographic key using the first and the second data further comprises the step of:

generating the cryptographic key using the first, second, third, and fourth data.

27. (Currently amended) The ~~computer-readable~~ computer storage medium of claim 25, wherein the computer-executable instructions further comprise the steps of:

determining a desired modulation scheme for wireless communications between the first host and the second host;

encrypting wireless data to be transmitted using the cryptographic key; and

transmitting the encrypted wireless data via the desired modulation scheme.

28. (Currently amended) The ~~computer-readable~~ computer storage medium of claim 25, wherein the computer-executable instructions further comprise the steps of:

determining a size of the cryptographic key;

monitoring an amount of data exchanged; and

selecting a final modulation scheme for a final data exchange between the first host and the second host such that an amount of data conveyed by the final modulation scheme added to the amount of data exchanged equals the size of the cryptographic key.

29. (Currently amended) The ~~computer-readable~~ computer storage medium of claim 25, wherein the step of:

selecting an initial modulation scheme comprises the step of:

sharing a short key established by a public key method, the short key providing an index to the initial modulation scheme.

30. (Currently amended) The ~~computer-readable~~ computer storage medium of claim 29, wherein the step of:

sharing a short key established by a public key method comprises the step of:

sharing a short key established by a Diffie-Hellman key exchange method.

31. (Currently amended) The ~~computer-readable~~ computer storage medium of claim 29, wherein the step of:

sharing a short key established by a public key method comprises the step of:

sharing a short key established using Kerberos.

32. (Currently amended) The ~~computer-readable~~ computer storage medium of claim 25, wherein the step of:

selecting an initial modulation scheme comprises the step of:

selecting an initial constellation.

33. (Currently amended) The ~~computer-readable~~ computer storage medium of claim 25, wherein the step of:

selecting an initial modulation scheme comprises the step of:

selecting an initial bit assignment for a constellation.

34-43. (Canceled)

44. (New) The method of claim 1, further comprising:

randomly selecting the second modulation scheme.

45. (New) The method of claim 1, wherein:

the first data comprises a first set of bits comprising at least one bit;

the second data comprises a second set of bits comprising at least one bit; and

generating the cryptographic key using the first and the second data comprises combining the first set of bits and the second set of bits.

46. (New) The method of claim 45, wherein combining the first set of bits and the second set of bits comprises concatenating the first set of bits and a the second set or bits.

47. (New) A method of wirelessly generating a cryptographic key that may be used to encrypt wireless communications between a first host and a second host, the first host and the second host comprising a wireless interface supporting communication using a plurality of modulation schemes, each modulation schemes of the plurality of modulation schemes encoding a number of bits per symbol, with the number of bits being different for different modulation schemes of the plurality of modulation schemes, the method comprising the steps of:

for each of a plurality of iterations, communicating a message between the first host and the second host using a modulation scheme, the message communicating a set of bits and a subsequent modulation scheme, the number of bits in the set of bits being based on the number of bits per symbol of the modulation scheme, and for each iteration after the first iteration, the modulation scheme being identified in a message communicated in a prior iteration; and

generating the cryptographic key using the sets of bits communicated in the plurality of iterations.

48. (New) The method of claim 47, further comprising:

selecting an initial modulation scheme for wireless transmission between the first host and the second host.

49. (New) The method of claim 48, wherein generating the cryptographic key comprises concatenating the sets of bits communicated in the plurality of iterations.

50. (New) The method of claim 47, further comprising:

for each of the plurality of iterations, randomly selecting the subsequent modulation scheme.

51. (New) The method of claim 47, further comprising:

for each iteration, generating the set of bits on one of the first host or the second host.